RFP

First Hit Fwd Refs

□ Generate Collection Print

L4: Entry 3 of 11 File: USPT Jan 8, 2002

US-PAT-NO: 6338050
DOCUMENT-IDENTIFIER: US 6338050 B1

TITLE: System and method for providing and updating user supplied context for a negotiations system

DATE-ISSUED: January 8, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Conklin; Jeffrey	Boston	MA		
Foucher; David	Somerville	MA		
Foucher; Daniel	Bedford	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Trade Access, Inc.	Boston	MA			02

APPL-NO: 09/ 192729 [PALM]
DATE FILED: November 16, 1998

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/80; 705/26
US-CL-CURRENT: 705/80; 705/26

FIELD-OF-SEARCH: 705/80, 705/1, 705/26, 705/27, 705/39, 705/37

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	4799156	January 1989	Shavit et al.	
□	5195031	March 1993	Ordish	364/403
□	5253165	October 1993	Leiseca et al.	
□	5305200	April 1994	Hartheimer et al.	
□	5495412	February 1996	Thiessen	364/401
□	5557518	September 1996	Rosen	

□	5629982	May 1997	Micali	
□	5666420	September 1997	Micali	
□	5671279	September 1997	Elgamal	
□	5677955	October 1997	Doggett et al.	
□	5692206	November 1997	Shirley et al.	395/793
□	5715314	February 1998	Payne et al.	
□	5732400	March 1998	Mandler et al.	
□	5757917	May 1998	Rose et al.	
□	5787262	July 1998	Shakib et al.	395/200.35
□	5787402	July 1998	Potter et al.	705/37
□	5790677	August 1998	Fox et al.	
□	5794207	August 1998	Walker et al.	
□	5802497	September 1998	Manasse	
□	5809144	September 1998	Sirbu et al.	
□	5826244	October 1998	Huberman	705/37
□	5873071	February 1999	Ferstenberg et al.	705/37
□	5897621	April 1999	Boesch et al.	705/26
□	5905975	May 1999	Ausubel	705/37
□	5918218	June 1999	Harris et al.	705/37
□	5924082	July 1999	Silverman et al.	705/37
□	5963923	October 1999	Garber	705/37
□	6014643	January 2000	Minton	705/37
□	6067531	May 2000	Hoyt et al.	705/35
□	6141653	October 2000	Conklin et al.	705/80

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
WO 97/04410	February 1997	WO	

OTHER PUBLICATIONS

"Trade'ex Introduces E-Commerce Software for Procurement, Distribution, Virtual E-Markets," Business Wire, p. 04281405, Apr. 1998.*
Gibson, Stan, "10 Who Dared to Be Different," PC Week, p. 21, Jan. 1997.*
"Pioneering Reseller Sites," Computer Reseller News, No. 711, p. 206, Nov. 1996.*
"Trade'ex Develops Java Compliant Electronic Commerce Solution for Creating Wholesale Markets Over the Internet," Internet Content Report, vol. 1, No. 12, Sep. 1996.*
"Trade'ex Unveils MarketMaker Software for Creating Online Marketplace," Business Wire, p. 04280202, Apr. 1998.*
"Corporate EFT Report," Technology Center, vol. 18, No. 2, p. N/A, Feb. 1998.*
"TradeAccess Sponsors First U.S. Trade Mission Web Site For Department of

Commerce," PR Newswire, Dec. 1997.*
Jones, Chris, "Trade'ex Readies Java-based MarketMaker," InfoWorld, vol. 18, No. 44, p. 6, Oct. 1996.*
TDS Marketing Group, "Trade'ex Connects the UK," M2 Presswire, p. N/A, Oct. 1996.*
Schmerken, Ivy, "NASDAQ Revamps to Keep Up," Wall Street Computer Review, vol. 8, No. 10, p. 35(6), Jul. 1991.

ART-UNIT: 2163

PRIMARY-EXAMINER: Hafiz; Tariq R.

ASSISTANT-EXAMINER: Meinecke-Diaz; Susanna

ATTY-AGENT-FIRM: Stretch; Maureen

ABSTRACT:

A multivariate negotiations engine for international transaction processing which: enables a sponsor to create and administer a community between participants such as buyers and sellers having similar interests; allows a buyer/participant to search and evaluate seller information, propose and negotiate orders and counteroffers that include all desired terms, request sample quantities, and track activity; allows a seller/participant to use remote authoring templates to create a complete Website for immediate integration and activation in the community, to evaluate proposed buyer orders and counteroffers, and to negotiate multiple variables such as prices, terms, conditions etc., iteratively with a buyer. The system provides secure databases, search engines, and other tools for use by the sponsor, which enable the sponsor to define the terms of community participation, establish standards, help promote the visibility of participating companies, monitor activity, collect fees, and promote successes. All this is done through a multivariate negotiations engine system operated at the system provider's Internet site, thus requiring no additional software at the sponsors', or participant sellers', or buyer's sites. This also allows buyers and sellers to use and negotiate payment options and methods that are accepted internationally. The system maintains internal databases that contain the history of all transactions in each community, so that sponsors, buyers and sellers may retrieve appropriate records to document each stage of interaction and negotiation. Documents are created by the system during the negotiation process.

54 Claims, 61 Drawing figures

First Hit Fwd Refs

□ Generate Collection Print

L4: Entry 2 of 11 File: USPT Mar 26, 2002

US-PAT-NO: 6363365
DOCUMENT-IDENTIFIER: US 6363365 B1

TITLE: Mechanism for secure tendering in an open electronic network

DATE-ISSUED: March 26, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kou; Weidong	Scarborough			CA

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corp.	Armonk	NY			02

APPL-NO: 09/ 207094 [PALM]
DATE FILED: December 7, 1998

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/64; 705/78, 705/37, 705/26
US-CL-CURRENT: 705/64; 705/26, 705/37, 705/78

FIELD-OF-SEARCH: 705/1, 705/50-77, 705/26, 705/64, 705/74, 705/75, 705/78, 705/37

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	4458109	July 1984	Mueller-Schloer	178/22.11
□	5491750	February 1996	Bellare et al.	380/21
□	5638446	June 1997	Rubin	380/25
□	5850442	December 1998	Muftic	380/21
□	6014644	January 2000	Erickson	705/37
□	6055518	April 2000	Franklin et al.	705/37
□	6161099	December 2000	Harrington et al.	705/37

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
2332833	June 1999	GB	

OTHER PUBLICATIONS

Michiharu Kudo, Secure Electronic Sealed-Bid Auction Protocal with Public Key Cryptography,IEICE Trans. Fundamentals. vol. E81-A,No. 1 Jan. 1198.*
Bruce Schneier, Applied Cryptography, Second Edition, 1996, John Wiley & Sons,Inc,Chapter 24.5,Kerberos, pp. 566-571.*
"Secure Electronic Sealed-Bid Auction Protocol with Public Key Cryptography", By, Michiharu Kudo, Tokyo Research Laboratory, IBM Japan.

ART-UNIT: 2161

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Greene; Daniel

ATTY-AGENT-FIRM: Clay; A. Bruce Carstens, Yee & Cahoon

ABSTRACT:

A mechanism for securing bid proposals until close of tendering is provided for an electronic tendering system over an open network. In order to be permitted to file a bid electronically in response to an invitation to tender, prospective vendors encrypt their bid proposals using session keys obtained from a third party source. The encrypted proposals are filed with the bid requester who does not have access to the session keys while the tendering period remains open. The encrypted bid proposals are cached in a safe repository until close of tendering. In one embodiment, the bid requester itself holds onto the encrypted proposals, and obtain the session keys for accessing their contents from the third party on expiry of the bid submission period. In another embodiment, the bid requester double-encrypts each encrypted bid proposal as it is received using its own privately-held key, and forwards the double-encrypted proposals to the third party to hold in a safe repository until the close of tendering. The third party then returns the double-encrypted proposals to the bid requester along with the session keys to permit the bid requester to access their contents. In either case, the party that caches the bid proposals until the close of tendering does not have access to the key required to decrypt the proposals.

15 Claims, 4 Drawing figures

First Hit Fwd Refs

□ Generate Collection Print

L4: Entry 2 of 11 File: USPT Mar 26, 2002

DOCUMENT-IDENTIFIER: US 6363365 B1
TITLE: Mechanism for secure tendering in an open electronic network

Abstract Text (1):
A mechanism for securing bid proposals until close of tendering is provided for an electronic tendering system over an open network. In order to be permitted to file a bid electronically in response to an invitation to tender, prospective vendors encrypt their bid proposals using session keys obtained from a third party source. The encrypted proposals are filed with the bid requester who does not have access to the session keys while the tendering period remains open. The encrypted bid proposals are cached in a safe repository until close of tendering. In one embodiment, the bid requester itself holds onto the encrypted proposals, and obtain the session keys for accessing their contents from the third party on expiry of the bid submission period. In another embodiment, the bid requester double-encrypts each encrypted bid proposal as it is received using its own privately-held key, and forwards the double-encrypted proposals to the third party to hold in a safe repository until the close of tendering. The third party then returns the double-encrypted proposals to the bid requester along with the session keys to permit the bid requester to access their contents. In either case, the party that caches the bid proposals until the close of tendering does not have access to the key required to decrypt the proposals.

Application Filing Date (1):
19981207

Brief Summary Text (23):
Another object of the invention is to provide an electronic tendering system in which: 1. the party requesting tenders (eg., a government agency) cannot see the contents of bid proposals until the tender is closed; 2. a third party holding the submitted bids does not see the bid proposals at all where the third party is not a trusted third party; and 3. no vendor (bidder) can see the content of any other vendor's bid proposal.

Brief Summary Text (24):
In accordance with these and other objects, the invention provides a lock box mechanism for safely storing electronic bid proposals submitted by vendors during open tendering over a network. The mechanism consists of the following elements: (i) a first encryption key shared only between a vendor and a third party authenticator during the open tendering which is used by the vendor for transforming a bid proposal to an inaccessible form prior to submitting the bid proposal to a bid requester, (ii) means held privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor, and (iii) an electronic repository for storing the submitted bid proposal until expiry of the open tendering. According to one aspect, the bid requester has direct access to the electronic repository while the third party authenticator does not, and preferably, the bid requester notifies the third party authenticator of receipt of bid proposals. According to another aspect, the third party authenticator has access to the electronic repository and the bid requester does not. Then, preferably, the bid requester double-encrypts bid

proposals it receives using its privately-held encryption key, and forwards the double-encrypted bid proposals on to the third part authenticator for storage.

Brief Summary Text (25):
The invention also provides a method for providing secure electronic tendering in an open network. On the bid requester's side, this method consists of publishing an invitation to tender electronic bid proposals (the invitation includes a requirement to encrypt bid proposals prior to submission using encryption keys generated from a specified authentication source), receiving encrypted bid proposals and rendering their contents inaccessible to the specified authentication source, and, on closure of the tendering, obtaining the encryption keys from the specified authentication source for accessing the bid proposals, On the side of the third pat authenticator, the method consists of generating an encryption key to a vendor for encrypting a bid proposal to be submitted by the vendor to the bid requester in response to a request, maintaining the vendor encryption key secret until notified of expiry of the open tender, and on the expiry of the open tender, forwarding the encryption key to the bid requester.

Detailed Description Text (4):
For example, a commercial tendering system for a large organisation is described in commonly assigned application titled "A Token-Based Deadline Enforcement System for Electronic Document Submission", and filed in the Canadian Patent Office on Jan. 30, 1998, as Application No. 2,228,331, (IBM docket number CA998-003). In that system, a master buyer server operating under a Microsoft Windows NT.RTM. operating system collects purchase requisitions from inside the bid requesting organisation, stores the requirements on a document information gateway operating under an IBM RS/6000.RTM. operating system behind a gateway with a firewall that protects the network within the organisation from the external network. Communications with suppliers and third party authenticators are handled by security software which automatically builds a secure structure before forwarding a message to a supplier over the network, and unpacks the secure structures it receives from the network in order to forward plain messages to other components on the internal network to process. The master buyer server publishes invitation; to tender on a tender bulletin board that includes software able to notify external parties (i.e., potential suppliers/vendors) of calls for tender. The vendors make bid submissions to the system using submission software operating on PC operating systems with network/Internet access, such as IBM OS/2.RTM. Warp, Microsoft Windows.RTM. 95, etc. Third party authenticators have similar support.

Detailed Description Text (6):
Thus, in response to the bid requester 102 issuing an invitation to tender (step 1), vendors 100 respond by indicating an intention to submit a tender and requesting authentication to do so (step 2). The bid requester 102 passes each authentication request on to the third party authenticator 104 (step 3), which in turn provides each vendors authentication directly back to that vendor 100 (step 4) or indirectly through the bid requester (not shown). Vendors 100 can then use their authentications to submit their bid proposals to the bid requester 102 (step 5). These proposals are kept in a bid cache 106, that could be located either with the bid requester 102 or the third party 104, until the closing day of the tender. However, neither the bid requester 102 or the third party 104 will have enough information to see the contents of the cached tenders, and no vendor has access to the content of any other vendor's bid submission. After the tender submission deadline has passed and all tenders have been received in the cache 106, the third party 104 sends the bid requester 102 its information on the tenders, which could constitute the encrypted tenders themselves if the third party hosts the cache (step 7), to enable the bid requester 102 to open all bid proposals and selects the successful tender (step 8).

Detailed Description Text (10):
A vendor who wishes to respond to the invitation to tender first makes a request to

the bid requester for a bid proposal identifier by electronically sending the bid requester a REQUEST_ID message (block 202). The message contains the date and the vendor's digital signature.

Detailed Description Text (11):
On receipt of the vendor's REQUEST_ID message, the bid requester attempts to verify the vendor's digital signature and date information (block 204). Failure to do so results in an error message being returned to the vendor (block 206). If the signature and date verify, the bid requester registers the vendor by generating a proposal identifier (block 208), which it sends to the third pat authenticator asking for a session key that will be used for encrypting the vendor's bid proposal (block 208). This vendor's session key is a shared secret between the vendor and the third party until the tender submission deadline has passed and tendering is closed.

Detailed Description Text (13):
The vendor receives the REGISTERED_ID message generated for it to obtain a proposal identifier, and verifies the digital signature and date information. If the message is from the third party directly (block 230), then this verification is for the third party's signature and date information only (block 232, else go to block 234 and return an error message to the third party). On the other hand, if forwarded by the requester (block 224), then both lie third party's and requester's signatures and date information should be verified. (Blocks 226, else go to block 238 and return an error message to the bid requester). If the signature(s) and date information verify, the vendor then decrypts the encrypted session key provided originally by the third party, by using its public key (block 236). The vendor generates a bid proposal or tender incorporating into it the proposal identifier (block 239, and encrypts the proposal using the session key (block 240). The encrypted proposal message is dated and digitally signed by the vendor, and returned to the bid requester which, on receipt, first verifies the date and signature information (block 242, else go to block 244 and return an error message to the vendor). Since the bid requester does not have the session key, it cannot read the vendor's bid proposal at this time.

Detailed Description Text (15):
Referring first to FIG. 3A, after verifying the date and vendor's digital signature contained in the proposal message, the bid requester generates a separate session key, called a requester session key, and encrypts the proposal again. The requester's session key will not be shared with anyone else, and it will be kept secretly by the bid requester itself. A message containing the double-encrypted proposal is dated and digitally signed by the bid requester, and forwarded to the third party (block 300) which verifies the date and bid requester's digital signature (block 302, else go to block 304 and return an error message to the bid requester). In the preferred embodiment, after verifying the date and digital signature contained in the double-encrypted proposal message, the third party forwards evidence of receipt of the proposal directly to the vendor. It should be noted that other systems could be employed for notifying the vendor of timely bid receipt, including sending the receipt directly from the bid requester to the vendor. A token-based system, where the vendor obtains a time-sensitive token to attach to the bid proposal prior to submitting it, is the subject matter of the above referenced IBM application for "A Token-Based Deadline Enforcement System for Electronic Document Submission";

Detailed Description Text (16):
Once the bid requester's signature and date information have been verified (block 302), the third party stores the proposal in a safe repository or cache until the tender close date (block 308).

Detailed Description Text (17):
After the deadline for tender submissions has expired, the bid requester generates

an ACCESS_REQUEST message (block 310) which it sends to the third party to require the proposals to be delivered. The third party encrypts the vendor's session key using the bid requester's public encryption key (block 312), and attaches the encrypted session key to the double-encrypted proposal (block 314). An ACCESS_GRANTED message with the encrypted session key attached to the double-encrypted proposal is dated and digitally signed by the third party, and returned to the bid requester (block 316).

Detailed Description Text (18):
After verifying the date and third party signature (block 318, else go to block 320 and return an error message to the third party), the bid requester uses its own private key to decrypt the vendor's session key which was formerly shared only by the vendor and third party (block 322), and which was encrypted by the third party using the bid requester's public key (as discussed in relation to block 312). The bid requester then uses the decrypted vendor's session key together with its own secret session key to decrypt the vendor's bid proposal (block 124).

Detailed Description Text (22):
After verifying the date and digital signature contained in the proposal message developed following the method of FIG. 2, the bid requester generates a PROPOSAL_RECEIVED message on the encrypted proposal received from the vendor using the proposal identifier and date information of that proposal (block 350). The bid requester digitally signs the PROPOSAL_RECEIVED message, and sends it to the third party (block 354), while storing the encrypted bid proposal in its own cache (block 352). It should be noted that the bid requester does NOT send a copy of the actual encrypted proposal to the third party which holds the vendor's session key for decrypting the proposal. Thus, the third party has no access to the encrypted bid proposal even though it shares the encryption key with the vendor.

Detailed Description Text (23):
After verifying the date and digital signature contained in the PROPOSAL_RECEIVED message (block 356, else go to block 358 and return an error message to the bid requester), the third party forwards evidence of bid receipt to the vendor (block 360) and keeps the PROPOSAL_RECEIVED message in a safe repository for a future non-repudiation purpose (block 362).

Detailed Description Text (24):
After expiry of the tender submission date, the bid requester sends a KEYREQUEST message to the third party to require the vendor's session key to access the vendor's encrypted proposal (block 364). The third party encrypts the session key shared between the it and the vendor, by using the bid requester's public encryption key (block 366). A KEY_GRANTED message containing the encrypted session key and the third party's digital signature is sent to the bid requester (block 368).

Detailed Description Text (25):
After verifying the date and third party signature in the KEY_GRANTED message (block 370, else go to block 372 and return an error message to the third party), the bid requester uses its own private key to decrypt the encrypted vendor's session key which was formerly shared only by the vendor and third party (block 374), and which was encrypted by the third party using the requester's public key (as discussed in relation to block 366). The bid requester then uses the decrypted vendor's session key to decrypt the vendor's bid proposal (block 376).

Current US Cross Reference Classification (1):
705/26

CLAIMS:

1. An electronic lock box mechanism for safely storing electronic bid proposals

submitted by vendors during open tendering over a network, comprising: a first encryption key shared only between a vendor and a third party authenticator during the open tendering, said encryption key being used by the vendor for transforming a bid proposal to an inaccessible form prior to submitting the bid proposal to a bid requester; means held privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor; and an electronic repository for storing the submitted bid proposal until expiry of the open tendering.

2. An electronic lock box mechanism, according to claim 1, wherein the means held privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor comprises: direct access to the electronic repository for storing and retrieving bid proposals; and means for notifying the third party authenticator on receipt and storage of the bid proposal; and wherein the third party authenticator does not have access to the electronic repository.

3. An electronic lock box mechanism, according to claim 2, further comprising means held by the bid requester for retrieving the bid proposal from the electronic repository and obtaining the first encryption key from the third party authenticator on the expiry of the open tendering.

4. An electronic lock box mechanism, according to claim 1, wherein the means held privately by the requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor comprises: a second encryption key held privately by the bid requester for encrypting the transformed proposal submitted by the vendor; and means for forwarding the double-encrypted proposal to the third party authenticator for storage until the expiry of the open tendering; and wherein the third party authenticator has access to the electronic repository for storing and retrieving bid proposals.

5. An electronic lock box mechanism, according to claim 4, further comprising means held by the third party authenticator for retrieving the double-encrypted proposal from the electronic repository, attaching the first encryption key to the double-encrypted proposal to form a message, and forwarding the message to the bid requester, on the expiry of the open tendering.

6. A method, implemented by a bid requesting party, for providing secure electronic tendering in an open network, comprising: publishing an invitation to tender electronic bid proposals, said invitation including a requirement to encrypt bid proposals prior to submission using encryption keys generated from a specified authentication source; receiving encrypted bid proposals and rendering their contents inaccessible to the specified authentication source; and on closure of the tendency, obtaining he encryption keys from the specified authentication source for accessing the bid proposals.

9. A method, implemented by an authentication party, for providing security in an open tender initiated by a bid requester, comprising: in response to a request, generating an encryption key to a vendor for encrypting a bid proposal to be submitted by the vendor to the bid requester; maintaining the vendor encryption key secret until notified of expiry of the open tender; and on the expiry of the open tender, forwarding the encryption key to the bid requester.

10. A method, according to claim 9, further comprising: caching the bid proposal received from the bid requester, said bid proposal being doubly-encrypted with the key generated to the vendor and a private encryption key of the bid requester; and on the expiry of the open tender, returning the bid proposal attached to the vendor encryption key to the bid requester.

11. A computer program product recorded on computer readable media for safely

storing electronic bid proposals submitted by vendors during open tendering over a network, comprising: computer readable means for sharing a first encryption key only between a vendor and a third party authenticator during the open tendering, said encryption key being used by the vendor for transforming a bid proposal to an inaccessible form prior to submitting the bid proposal to a bid requester; computer readable means held privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor; and computer readable electronic repository means for storing the submitted bid proposal until expiry of the open tendering.

12. The computer program product,according to claim 11, wherein the computer readable means hold privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor comprises: computer readable means for directly accessing the electronic repository for storing and retrieving bid proposals; and computer readable means for notifying the third party authenticator on receipt and storage of the bid proposal;

and wherein the third party authenticator does not have access to the electronic repository.

13. The computer program product according to claim 12, further comprising computer readable means held by the bid requester for retrieving the bid proposal from the electronic repository and obtaining the first encryption key from the third party authenticator on the expiry of the open tendering.

14. The computer program product according to claim 11, wherein the computer readable means hold privately by the bid requester for rendering the bid proposal inaccessible to the third party authenticator following submission by the vendor comprises: a second computer readable encryption key means held privately by the bid requester for encrypting the transformed proposal submitted by the vendor; and computer readable means for forwarding the double-encrypted proposal to the third party authenticator for storage until the expiry of the open tendering;

and wherein the third party authenticator has access to the electronic repository for storing and retrieving bid proposals.

15. The computer program product according to claim 14, further comprising computer readable means held by the third party authenticator for retrieving the double-encrypted proposal from the electronic repository, attaching the first encryption key to the double-encrypted proposal to form a message, and forwarding the message to the bid requester, on the expiry of the open tendering.

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs
Generate OACS

Search Results - Record(s) 1 through 10 of 11 returned.

□ 1. Document ID: US 6418415 B1
L4: Entry 1 of 11 File: USPT Jul 9, 2002

US-PAT-NO: 6418415
DOCUMENT-IDENTIFIER: US 6418415 B1
**** See image for Certificate of Correction ****

TITLE: System and method for aggregating multiple buyers utilizing conditional purchase offers (CPOS)

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

☑ 2. Document ID: US 6363365 B1
L4: Entry 2 of 11 File: USPT Mar 26, 2002

US-PAT-NO: 6363365
DOCUMENT-IDENTIFIER: US 6363365 B1

TITLE: Mechanism for secure tendering in an open electronic network

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 3. Document ID: US 6338050 B1
L4: Entry 3 of 11 File: USPT Jan 8, 2002

US-PAT-NO: 6338050
DOCUMENT-IDENTIFIER: US 6338050 B1

TITLE: System and method for providing and updating user supplied context for a negotiations system

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 4. Document ID: US 6336105 B1
L4: Entry 4 of 11 File: USPT Jan 1, 2002